疑似平方数に基づいた素数判定アルゴリズム (代数系および計算機科学基礎)

AUTHOR(S):

桑木, 康佑; 神保, 秀司

CITATION:

桑木, 康佑 ...[et al]. 疑似平方数に基づいた素数判定アルゴリズム (代数系および計算機科学基礎). 数理解析研究所講究録 2012, 1809: 65-72

ISSUE DATE:

2012-09

URL:

http://hdl.handle.net/2433/194473

数理解析研究所講究録
第1809巻 2012年 65-72

疑似平方数に基づいた素数判定アルゴリズム

桑木 康佑　　神保 秀司
岡山大学大学院自然科学研究科

概要 素数とは，自分自身と1以外に正整数の約数をもたない1より大きい整数のことである．現在情報通信における機密保全のために公開鍵暗号が使われている．公開鍵暗号では与えられた正整数が素数であるか否かを判定する素数判定アルゴリズムは暗号鍵生成において重要な役割を演じている．本論文の目的は，Lukes らにより提案された疑似平方数と呼ばれる各素数に対応する正整数に基づいた確定的素数判定アルゴリズムの改良の可能性について実験的に調査検証することである．奇素数 p に対して疑似平方数と呼ばれる正整数 L_p が対応する．Lukes らの素数判定アルゴリズムでは，与えられた正整数 n が素数か否かを判定するために，$n < L_p$ を満たす奇素数 p を見付け，p 以下の各素数 p_i に対して n を法とした p_i の $(n-1)/2$ 乗を計算する．$p(n)$ で n 番目の素数を表す．ただし，最初の素数は，$p(1) = 2$ とする．$L_{p(n)}$ は n に対して指数関数的に増加すると予想されている．この予想が正しければ，APRT-CL 法や ECPP 法など現在使われている確定的素数判定アルゴリムよりも高速な素数判定が可能になる．本論文では，Lukes らによる疑似平方数に基づいた確定的素数判定アルゴリズムで使われている判定条件のうちの1つを取り除くことができる可能性を計算機実験により調査した．その結果，この条件判定はその素数判定アルゴリズムの引数がカーマイケル数である場合にのみ必要であるという予想が提案されている．

Algorithms for Primality Testing Based on Pseudosquares

Kosuke KUWAGI　and　Shuji JIMBO
Graduate School of Natural Science and Technology, Okayama University

ABSTRACT. A prime number is a positive integer greater than 1 that has no positive divisors other than 1 and itself. Public-key cryptography is used for confidentiality preservation in telecommunication today. In public-key cryptography, primality tests, that is algorithms to determine whether a given number is prime, are play important roles for public-key generation. The purpose of the research is to view and verify the possibility of an improvement of a primality test proposed by Lukes et al by experiments with computers. For each odd prime number p, a positive integer L_p called a pseudosquare corresponds to p. In the algorithm of Lukes et al, a prime number p with $n < L_p$ is found, then, to determine whether a given positive integer n is a prime number or not, for each prime number p_i less than or equal to p, a calculation of p_i raised, modulo n, to the power $(n-1)/2$ is made. Let $p(n)$ denote the n-th prime number, where $p_1 = 2$ is the first prime number. It is conjectured that the n-th pseudosquare $L_{p(n)}$ should grow exponentially in n. If the conjecture holds, then we can obtain a faster rigorous primality test than

APRT-CL test or ECPP test, which is used in practice today. In this research, possibility of removing one of primality conditions used in the rigorous primality test based on pseudosquares of Lukes et al. is investigated by computer experiments. In consequence, the following conjecture is proposed: The condition is needed only in the case where the argument of the primality test is a Carmichael number.

1 はじめに

素数 p に対する疑似平方数 L_p とは，次の2条件を満たす平方数でない最小の正整数である．

1. $L_p - 1$ は8の倍数であり，
2. $2 < q \leq p$ を満たすすべての素数 q について $L_p - m^2$ が q の倍数になるような正整数 m が存在する．

これらの条件を数式を使って書き直せば次のようになる．

1. $L_p \equiv 1 \pmod 8$,
2. $\exists m \in \mathbb{Z}^+,\ L_p \equiv m^2 \pmod q$

上の第2の条件を表す数式は平方剰余についての Legendre の記号を使って

$$\left(\frac{L_p}{q}\right) = 1$$

と表すことができる．この第2の条件のとおり，L_p は平方数ではないが，p 以下のどの素数を法としたときも平方数として振る舞う．

奇素数 p に対する関数値 L_p について，計算機実験の結果に基づいて L_p が p に対して指数関数的に増加することが予想されていて，Lukes らにより，この予想を前提とした高速な確定的素数判定アルゴリズムが提案されている [2]．一方，L_p の増加について ERH (拡張リーマン予想) を仮定した結果が得られているが，その増加傾向は上記の計算機実験の結果に基づいた予想よりも小さいオーダである．ERH の成立だけを仮定して得られる確定的素数判定アルゴリズムは，Miller らによる ERH を仮定した確定的素数判定アルゴリズムよりもそれほど速くはならない．

現代の情報通信において，巨大な2素数の積の因数分解が困難であるという予想などを前提とした RSA 公開鍵暗号が広く使われている．年々利用可能な計算機の能力と規模の増加に応じて RSA 公開鍵暗号が解読される危険性も高まるため，公開鍵の規模も時間とともに増加している．RSA 公開鍵暗号における公開鍵の作成では，公開鍵の規模に応じた巨大な新しい素数の生成が要求される．そのため，ランダムに選んだ巨大な整数を高速かつ確定的に素数判定するアルゴリズムの開発は，情報通信の効率化に寄与できると期待される．

これ以降，最初の素数を $p(1) = 2$ で表し，k 番目の素数を $p(k)$ で表す．本論文では，疑似平方数 $L_{p(n)}$ の n に対する指数関数的な増加の予想を前提として，Lukes らによる

確定的素数判定アルゴリズムの改良の可能性について計算機実験により調査した．Lukesらのアルゴリズムでは，2つの判定条件を確認しているが，そのうちの1つを省略した場合の振舞いについて検証し，その条件の必要性を確認した．さらに，誤判定が生じた判定対象の正整数についての調査に基づいて，上のように1つの条件を省略した場合カーマイケル数を素数判定したときのみ誤判定が生じるという予想を提案する．

第2節で，Lukesらによる疑似平方数に基づいた素数判定アルゴリズムを概観し，Lukesらのアルゴリズムの計算時間と L_p の増加の程度の関係について述べる．さらに，実際の計算結果により得られている疑似平方数 L_p の増加の様子と理論的に得られている L_p の上界と下界について概観する．第3節で，Lukesらのアルゴリズムの判定条件の1つを省略した場合に誤判定が生じる条件についての，カーマイケル数と呼ばれる数との関連性に着目した計算機実験の結果を示し，それに基づいてその条件を省略した場合の誤判定についての予想を提案する．第4節では，まとめと今後の課題を述べる．

2 疑似平方数に基づいた素数判定アルゴリズム

Lukesらは，与えられた奇数 n が素数であるための次の必要十分条件を与えた．

定理 1 n は1より大きい奇数であるとし，B は正整数であるとし，p は素数であるする．このとき，次の条件がすべて成り立てば，n は素数か，または，素数の累乗である．

(1) n の素因数は，すべて B より大きい．

(2) $n < BL_p$ が成り立つ．

(3) $q \leqq p$ を満たすすべての素数 q について $q^{(n-1)/2} \equiv \pm 1 \pmod{n}$ が成り立つ．

(4) $n \equiv 5 \pmod 8$ のとき $2^{(n-1)/2} \equiv -1 \pmod{n}$ が成り立ち，$n \equiv 1 \pmod 8$ のとき $r^{(n-1)/2} \equiv -1 \pmod{n}$ および $r \leqq p$ を満たす奇素数 r が存在する．

この定理1を使って与えられた1より大きい奇数 n が素数であることを決定するには，$n = a^b$ を満たす1より大きい整数 a, b が存在しないことを示す必要がある．例えば，2以上かつ n の2進桁数以下である各素数 d について，近似計算法のニュートン法を使って $c = \lfloor \sqrt[d]{n} \rfloor$ を計算し，さらに $n = c^d$ を判定することにより，$n = a^b$ を満たす1より大きい整数 a, b が存在するかしないかを決定することができる．また，定理1の条件を判定するには，Miller-Rabin法と同様に反復二乗法で $q^{(n-1)/2} \bmod n$，$r^{(n-1)/2} \bmod n$ を求めればよい．

オーダの記法の略記法として，$f(n) = \tilde{O}(g(n))$ で $f(n) = O(g(n)(\log g(n))^m)$ を満たす正整数 m が存在することを表す．定理1に現れる定数 B の値は，実質的アルゴリズム全体の計算時間のオーダに影響しないと考えられるため，以下 $B = 1$ と仮定する．さらに，与えられた正整数 n に対して，$n < L_{p(k)}$ を満たす最小の正整数 k を $k(n)$ で表すことにする．

入力 n に対する定理1に基づいたアルゴリズムの計算時間を $T(n)$ で表し，n のサイズ (2進桁数) を $l(n)$ で表したとき，上の考察より

$$T(n) = \tilde{O}(k(n)(l(n))^2)$$

が成り立つことが導かれる．詳細は省略する．現在得られている k と $L_{p(k)}$ の値の組合せのいくつかを表 1 に挙げる．特に，$L_{p(k)}$ の値が正確に求まっている k の最大値は，$k = 74$ である [4]．現在までに知られている k と L_p の対応関係に裏付けられた $k(n) = O(l(n))$ という予想が提案されている [2][5][4]．この予想が成り立てば，$T(n) = \tilde{O}((l(n))^3)$ が成り立ち，さらに，この予想のオーダにおける $l(n)$ の係数が比較的小さいことも予想されているので，定理 1 に基づいたアルゴリズムは現在使用されている確定的素数判法である APRT-CL 法や ECPP 法と比較しても実用上高速である．

表 1: 現在得られている疑似平方数 $L_{p(k)}$ の抜粋

k	$p(k)$	$L_{p(k)}$	k	$p(k)$	$L_{p(k)}$
1	2	17	40	173	178936222537081
2	3	73	50	229	196640148121928601
3	5	241	60	281	208936365799044975961
4	7	1009	70	349	99429945930479213334049
10	29	117049	72	359	295363187400900310880401
20	71	427733329	73	367	365533442947705746004 6489
30	113	196265095009	74	373	42350252230805975035 19329

現在，疑似平方数 L_p の上界と下界について，Schinzel によって次の 2 つの定理が得られている [3]．

定理 2 任意の $\varepsilon > 0$ に対して，$p_0(\varepsilon)$ が存在し，任意の $p > p_0(\varepsilon)$ に対して次の不等式が成り立つ．

$$p^{4\sqrt{e}-\varepsilon} < L_p < e^{((1/4)+\varepsilon)p}$$

定理 3 拡張リーマン予想 (ERH) を仮定すれば，任意の $\varepsilon > 0$ に対して，$p_0(\varepsilon)$ が存在し，任意の $p > p_0(\varepsilon)$ に対して次の不等式が成り立つ．

$$e^{(1-\varepsilon)\sqrt{p}} < L_p < e^{(2\log_2 2+\varepsilon)(p/\log_2 p)}$$

3 疑似平方数に基づいた素数判定条件とカーマイケル数

この節では，素数の累乗でない合成数 n を定理 1 によって合成数であると判定する場合の条件 (4) の必要性について検討する．与えられた奇数 n が条件 (1), (2), (3) をすべて満たしているとき，$n \equiv 3 \pmod 4$ が成り立っていれば，直ちに n が素数かまたは素数の累乗であることが導かれる．そうでないとき，定理 1 に従って n が素数かまたは素数の累乗であることを示すには，条件 (4) が成り立つか否かを判定しなくてはならない．

与えられた奇数 n について $n \equiv 1 \pmod 4$ が成り立っている場合の条件 (4) の必要性を調べるために，$B = 1$ とおいて次の条件 A を満たす正整数 n の存在を計算機実験により調査した．実験で使ったプログラムの作成には，プログラミング言語として C を採用し，Gnu MP (GMP) ライブラリを利用した．

条件 A $p = p(k(n))$ とおいたとき，n は，条件 (3) を満たし，かつ，異なる素因数をもつ (単一の素因数の累乗でない) 合成数である．

$p = p(k(n))$ は，$n < L_p$ ($B = 1$ を仮定した場合の条件 (2)) を満たす最小の素数である．また，n が条件 A を満たすためには，$2^{(n-1)/2} - 1$ が n の倍数でなくてはならないので，n は奇数でなくてはならない．

この実験の結果，$n < 10^7$ の範囲で条件 A を満たす奇数 n は，次の 5 つであることが判明した．

$$488881, \quad 3057601, \quad 3828001, \quad 6189121, \quad 9439201$$

条件 A を満たす n が無限に存在すれば，定理 1 に基づいた素数判定アルゴリズムから単純に条件 (4) を省くことはできない．条件 A を満たす n が無限に存在する可能性を検討するために，上の 5 つの奇数を素因数分解したところ，すべてカーマイケル数 (Carmichael number) であることが判明した．

$$\begin{aligned} 488881 &= 37 \cdot 73 \cdot 181 \\ 3057601 &= 43 \cdot 211 \cdot 337 \\ 3828001 &= 101 \cdot 151 \cdot 251 \\ 6189121 &= 61 \cdot 241 \cdot 421 \\ 9439201 &= 61 \cdot 271 \cdot 571 \end{aligned}$$

正整数 n がカーマイケル数であるとは，$1 < a < n$ および $\gcd(a, n) \neq 1$ を満たすすべての整数 a について

$$a^{n-1} \equiv 1 \pmod{n}$$

が成り立つことである．カーマイケル数について次の定理が知られている．

定理 4 次の条件は，合成数 n がカーマイケル数であるための必要十分条件である．

> n のすべての素因数 p に対して，$p - 1 \mid n - 1$ ($n - 1$ は $p - 1$ の倍数である)
> および $p^2 \nmid n$ (n は p^2 の倍数でない) が成り立つ．

上に挙げた条件 A を満たし，かつ，10^7 より小さい 5 つの合成数の素因数分解と定理 4 から，これら 5 つの合成数がすべてカーマイケル数であることが導かれる．さらに n を 10^{12} 未満の 8241 個のカーマイケル数について条件 A の成立を調べたところ，条件 A を満たすものが 517 個存在することが判明した．興味深いのは，これら 517 個のうち 8 を法として 5 と合同であるものが 6236982181, 43025053501, 613976914981 の 3 つのみであることである．

n をカーマイケル数とし，その素因数分解を $n = p_1 p_2 \cdots p_m$，$p_1 < p_2 < \cdots < p_m$，で表す．オイラーの基準

$$\left(\frac{a}{p_i}\right) \equiv a^{(p_i-1)/2} \pmod{p_i}$$

より，各 p_i の倍数でない任意の正整数 a について

$$a^{(p_i-1)/2} \equiv \pm 1 \pmod{p_i}$$

が成り立つ．従って，$p = p(k(n))$ ($n < L_p$ を満たす最小の素数) とおいたとき，次の2条件が成り立てば，n は条件 A を満たすことが中国剰余定理を使って容易に示すことができる．

条件 B1 $p < p_1$,

条件 B2 $\forall q \in \{p(1), p(2), \ldots, p(k(n))\}$, $\forall i \in \{1, 2, \ldots, m\})(q^{(p_i-1)/2} \equiv 1 \pmod{p_i})$,
または，$\forall q \in \{p(1), p(2), \ldots, p(k(n))\}$, $\forall i \in \{1, 2, \ldots, m\})(q^{(p_i-1)/2} \equiv 1 \pmod{p_i})$.

条件 B1 および B2 を満たすカーマイケル数を見付けるために，次のカーマイケル数を導く多項式 $U_3(m)$ に着目する [1].

定理 5 任意の正整数 m に対して，$6m+1$，$12m+1$，および $18m+1$ がすべて素数であるなら，

$$U_3(m) = (6m+1)(12m+1)(18m+1)$$

はカーマイケル数である．

$4\sqrt{e} > 6$ であり，かつ，任意の $m \geqq 2$ について $(3m)^6 > U_3(m)$ が成り立つ．$6m+1$ が素数であるなら $3m$ 以上 $6m+1$ 未満である素数が存在するので，定理 2 より，十分大きい m について，$6m+1$，$12m+1$，および $18m+1$ がすべて素数であるならば，$U_3(m)$ はカーマイケル数であり，かつ，$n = U_3(m)$ が条件 B1 を満たすことが導かれる．

$6m+1$，$12m+1$，および $18m+1$ がすべて素数であり，$L_{p(73)} \leqq U_3(m) < L_{p(74)}$ および $p(74) < 6m+1$ を満たし，かつ，$n = U_3(m)$ が条件 B2 を満たす正整数 m を計算機実験により次のように探索した．このような m を見付けるには，$m_0 = 14128869$ とおき，$m_1 = 14839422$ とおいたとき，$U_3(m_0 - 1) < L_{p(73)} = L_{367} < U_3(m_0)$ および $U_3(m_1) < L_{p(74)} = L_{373} < U_3(m_1 + 1)$ が成り立ち，さらに，$p(74) = 373 < 84773215 = 6m_0 + 1$ が成り立つので，$m_0 \leqq m \leqq m_1$ を満たす整数 m で，$6m+1$，$12m+1$，$18m+1$ がすべて素数であり，かつ，$U_3(m)$ が条件 B2 を満たすものを探せばよい．

その結果，そのような整数 m は，1815 個存在することが判明した．そのうちの最小のものと最大のものを，それらに対応する $U_3(m)$ の値とともに下に挙げる．

$$m_{\min} = 14128946,\ U_3(m_{\min}) = 365539494380103287828344 9,$$

$$m_{\max} = 14839376,\ U_3(m_{\max}) = 423498550128100744968172 9.$$

一方，$m_0 \leqq m \leqq m_1$ の範囲の整数 m で $6m+1$，$12m+1$，$18m+1$ がすべて素数でありながら $U_3(m)$ が条件 B2 を満たさないものは，全く存在しないことが判明した．さらに，$6m+1$，$12m+1$，および $18m+1$ がすべて素数であり，かつ，$L_{p(73)} \leqq U_3(m) < L_{p(74)}$ を満たす整数 m と $1 \leqq k \leqq 74$ を満たす k の組 (m, k) すべてについて，

$$(p(k))^{U_3(m)-1} \equiv 1 \pmod{U_3(m)}$$

が成り立つことが判明した．

以上の議論に基づいて次の予想を提案する．

予想 1 $6m+1$, $12m+1$, および $18m+1$ がすべて素数であり，かつ，$n=U_3(m)$ が条件 B2 を満たす正整数 m が無限に存在する．

この予想が成り立てば，条件 A を満たす正整数 n が無限に存在することが直ちに導かれる．すなわち，Lukes らの素数判定アルゴリズムにおいて条件 (4) の判定を省略した場合，誤判定が生じる入力の奇数 n が無限に存在することをが導かれる．さらに，次の予想も加える．

予想 2 条件 A を満たす正整数は，すべてカーマイケル数である．

4 おわりに

第 2 節で導入した Lukes らの素数判定アルゴリズムにおいて条件 (4) の判定を省略すること自体は，計算時間の短縮にほとんど影響しないと考えられる．しかしながら，p_i が動く範囲が変化することを許した上で，条件 (3) の形の判定条件だけにすることができれば，アルゴリズムの構造がより簡潔になり改良のし易さにつながることが期待される．一方，予想 1 が成り立てば，単純に条件 (4) を省略することは困難である．さらに，予想 2 が成り立てば，条件 (4) は，素数判定アルゴリズムにおいてカーマイケル数の一部によって生じる誤判定を防止するためだけに存在すると考えることができる．

今後の課題としては，予想 1 の理論的証明を第一に挙げる．理論的考察を支援するために計算機実験をする場合，与えられた奇数 n に対する $p=p(k(n))$，すなわち，$n<L_{p(k)}$ を満たす最小の正整数 k を見付けることが困難なため，n についての条件 B2 を厳密に判定することが困難になることが問題になるかもしれない．その場合，条件 B2 を定理 2，定理 3 に基づいて緩く判定する形に修正するという対策が考えられる．

実用的な面からは，確定的素数判定の効率化が重要であり，定理 1 のような形の素数判定条件の改良が望ましい．これを第二の課題として挙げる．素数判定の対象の奇数 n の範囲を定数 N 以下に制限した場合，素数判定条件の改良が容易になり，実際の計算時間が従来のものよりも高速な確定的素数判定アルゴリズムの設計につながることが期待される．

謝辞

2012 年 2 月 20 日から同年 2 月 22 日に掛けて京都大学数理解析研究所で開催された「代数系および計算機科学基礎」研究集会での著者らによる発表において，活発に議論して頂いた聴衆の皆様に深く感謝致します．

参考文献

[1] J. Chernick. On Fermat's simple theorem. *Bull. Amer. Math. Soc*, Vol. 45, No. 269–274, p. 5, 1939.

[2] R. F. Lukes, C. D. Patterson, and H. C. Williams. Some results on pseudosquares. *Mathematics of computation*, Vol. 65, No. 213, pp. 361–372, 1996.

[3] A. Schinzel. On pseudosquares. *New Trends in Prob. and Stat*, Vol. 4, pp. 213–220, 1997.

[4] J. Sorenson. Sieving for pseudosquares and pseudocubes in parallel using doubly-focused enumeration and wheel datastructures. *Algorithmic number theory*, pp. 331–339, 2010.

[5] K. Wooding and H. C. Williams. Doubly-focused enumeration of pseudosquares and pseudocubes. *Algorithmic Number Theory*, pp. 208–221, 2006.